ADDRESSING THE HARM OF TOTAL SURVEILLANCE: A REPLY TO PROFESSOR NEIL RICHARDS

Danielle Keats Citron[*] *and David Gray*[**]

The ethos of our age is "the more data, the better."[1] In nearly every sector of our society, information technologies identify, track, analyze, and classify individuals by collecting and aggregating data. Law enforcement, agencies, industry, employers, hospitals, transportation providers, Silicon Valley, and individuals are all engaged in the pervasive collection and analysis of data that ranges from the mundane to the deeply personal.[2] Rather than being silos, these data gathering and surveillance systems are linked, shared, and integrated. Whether referred to as coveillance,[3] sousveillance,[4] bureaucratic surveillance,[5] "surveillance-industrial complex,"[6] "panvasive searches,"[7] or business intelligence, total-information awareness is the objective.[8]

[*] Lois K. Macht Research Professor of Law, University of Maryland School of Law; Affiliate Scholar, Stanford Center on Internet and Society; Affiliate Fellow, Yale Information Society Project.

[**] Associate Professor of Law, University of Maryland School of Law. We are grateful to Neil Richards for his thoughtful essay and feedback and to Julie Cohen, Leslie Henry, Amanda Pustilnik, Daniel Solove, and the participants in the *Harvard Law Review* Symposium on Privacy and Technology for their helpful suggestions.

[1] Kelley Stone, Deploying and Operating an Effective Regional Fusion Center: Lessons Learned from the North Central Texas Fusion System 6 (July 19, 2007) (unpublished manuscript) (on file with the Harvard Law School Library).

[2] *See, e.g.*, Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 19, 2012, at MM30.

[3] JULIE E. COHEN, CONFIGURING THE NETWORKED SELF 144–48 (2012).

[4] Steve Mann et al., *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1 SURVEILLANCE & SOC'Y 331 (2003) (describing personalized computer devices recording users' activities).

[5] JOHN GILLIOM, OVERSEERS OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY 18, 119 (2001) (exploring surveillance of the poor to administer public benefits).

[6] JAY STANLEY, AM. CIVIL LIBERTIES UNION, THE SURVEILLANCE-INDUSTRIAL COMPLEX: HOW THE AMERICAN GOVERNMENT IS CONSCRIPTING BUSINESSES AND INDIVIDUALS IN THE CONSTRUCTION OF A SURVEILLANCE SOCIETY (2004), *available at* http://www.aclu.org/FilesPDFs/surveillance_report.pdf (documenting industry's partnership with government to engage in monitoring of citizens).

[7] Christopher Slobogin, *Rehnquist and Panvasive Surveillance*, 82 MISS. L.J. 307 (2013).

[8] *See* Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 511, 121 Stat. 266, 317. *See generally* INFORMATION AND INTELLIGENCE (INCLUDING TERRORISM) FUSION CENTERS 5 (Todd Masse et al. eds., 2008).

Consider Virtual Alabama.[9] Google has built a customized database for Alabama's Department of Homeland Security that combines three-dimensional satellite/aerial imagery of the state with geospatial analytics that reveal relationships, trends, and patterns in incoming data.[10] Virtual Alabama can "track moving objects, monitor sensors, and overlay near-real time data sets."[11] Alabama will continue to add inputs,[12] but the system already aggregates data from traffic cameras, real-time private and public video streams, GPS location data for police cruisers, building schematics, sex offenders' addresses, and landownership records.[13] The state's 1500 public schools plan to link their video cameras into the system, providing live streaming 24 hours a day, 7 days a week.[14] Virtual Alabama is also encouraging contributions from government agencies in exchange for access to the system.[15] The stated goal of the program is to map all available data in the state.[16]

Virtual Alabama is part of a broader surveillance system sponsored by federal, state, and local governments and their private partners. In the wake of the 9/11 attacks, Congress adopted a number of innovations to break down ossified bureaucratic structures that previously impeded intelligence efforts to identify future threats. Among these innovations was the creation of the new Department of Homeland Security.[17] Amidst these efforts, the United States rejected proposals to establish an intelligence agency akin to Britain's MI5, which is devoted to domestic intelligence and surveillance, due to bureaucratic in-

---

[9] *See* TORIN MONAHAN, SURVEILLANCE IN THE TIME OF INSECURITY 47 (2010); *Google Earth Enterprise Case Study: Virtual Alabama*, YOUTUBE (Sep. 24, 2008), http://www.youtube.com/watch?v=a-1IoJTWiIY.

[10] MONAHAN, *supra* note 9, at 46–49.

[11] *2008 Innovation Awards Program Application*, COUNCIL ST. GOV'TS 1, http://ssl.csg.org/innovations/2008/2008Southapplications/08S05alvirtualalabama.pdf (last visited May 14, 2013).

[12] *Id.* at 3.

[13] Corey McKenna, *Virtual Alabama Facilitates Data Sharing Among State and Local Agencies*, DIGITAL COMMUNITIES (Aug. 13, 2009), http://www.digitalcommunities.com/articles/virtual-alabama-facilitates-data-sharing-among.html.

[14] Lamar Davis & Jacob Cook, *Virtual Alabama School Safety System*, http://rems.ed.gov/docs/fy10rems_fgm_nhmd_virtualalabama.pdf (last visited May 14, 2013). Some states require public school students to carry Radio Frequency Identification (RFID) cards that track their whereabouts. *"Smart" Student ID Cards: Student Locator Pilot*, NORTHSIDE ISD, http://www.nisd.net/studentlocator/ (last visited May 14, 2013) (describing Texas RFID program that tracks the location of students while at school).

[15] *Alabama's Layered Approach*, GCN (Oct. 17, 2008), http://gcn.com/articles/2008/10/17/alabamas-layered-approach.aspx?page=2.

[16] MONAHAN, *supra* note 9, at 46.

[17] Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1442 (2011).

fighting and fear of a civil liberties firestorm.[18] But what it eschewed formally, it pursued in fact.

Since 9/11, a surveillance state has been in development,[19] accomplished in part by a network of fusion centers through which government agents and private-sector representatives "collect and share" information and intelligence.[20] State- and locality-run fusion centers get most of their funding from federal grants.[21] Their stated goal is to detect and prevent "all hazards, all crimes, all threats."[22] At the Washington Joint Analytical Center, for instance, analysts from the Department of Homeland Security, the FBI, state police, and Boeing generate and analyze "criminal and anti-terrorism intelligence."[23]

Congressional panels, journalists, and citizens have been told that fusion centers raise few privacy concerns and that their information gathering is focused and valuable.[24] Contrary to these assurances, critics have argued that fusion centers erode civil liberties without concomitant gains for security.[25] A recent Congressional report backs these concerns, demonstrating that fusion centers have amounted to a waste of resources.[26]

Fusion centers cast a wide and indiscriminate net. Data-mining tools analyze a broad array of personal data culled from public- and private-sector databases, the Internet, and public and private video cameras. Fusion centers access specially designed data-broker databases containing dossiers on hundreds of millions of individuals, including their Social Security numbers, property records, car rentals, credit reports, postal and shipping records, utility bills, gaming, insurance claims, social network activity, and drug- and food-store records.[27] Some gather biometric data and utilize facial-recognition software.[28] On-the-ground surveillance is collected, analyzed, and shared as well. For example, the San Diego fusion center purchased

---

[18] Matthew C. Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, 3 J. NAT'L SECURITY L. & POL'Y 377, 405-07 (2009).

[19] Many observers argue that we already live in a surveillance state. *See, e.g.*, Jack M. Balkin, Essay, *The Constitution in the National Security State*, 93 MINN. L. REV. 1 (2008).

[20] Citron & Pasquale, *supra* note 17, at 1449 (exposing fusion centers as waste of resources and threat to civil liberties).

[21] *Id.*

[22] *Id.* at 1450.

[23] *Id.* (quoting Alice Lipowicz, *Boeing to Staff FBI Fusion Center*, WASH. TECH. (June 1, 2007), http://washingtontechnology.com/articles/2007/06/01/boeing-to-staff-fbi-fusion-center.aspx).

[24] *Id.* at 1443.

[25] *See, e.g.*, *id.* at 1443 n.5.

[26] *See* U.S. S. PERMANENT SUBCOMM. ON INVESTIGATIONS, MAJORITY AND MINORITY STAFF REPORT, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS (2012), *available at* http://cdn.govexec.com/media/gbc/docs/pdfs_edit/100312cc1.pdf [hereinafter MAJORITY AND MINORITY STAFF REPORT].

[27] *Id.*

[28] CITRON & PASQUALE, *supra* note 17, at 1451.

tiny cameras for law enforcement to attach to their shirt buttons, hats, and water bottles.[29] Through the federal government's "Information Sharing Environment,"[30] information and intelligence is distributed to public entities, including state, local, and federal agencies, and private owners of "critical infrastructure," such as transportation, medical, and telecommunications infrastructure.[31]

The scope of surveillance capacities continues to grow. Fusion centers and projects like Virtual Alabama may already have access to broadband providers' deep packet inspection (DPI) technologies, which store and examine consumers' online activities and communications.[32] This would provide government and private collaborators with a window into online activities,[33] which could then be exploited using data-mining and statistical-analysis tools capable of revealing more about us and our lives than we are willing to share with even intimate family members.[34] More unsettling still is the potential combination of surveillance technologies with neuroanalytics to reveal, predict, and manipulate instinctual behavioral patterns of which we are not even aware.[35]

There can be no doubt that advanced surveillance technologies such as these raise serious privacy concerns. In his article, Professor Neil Richards offers a framework to "explain why and when surveillance is particularly dangerous and when it is not."[36] Richards contends that surveillance of intellectual activities is particularly harmful because it can undermine intellectual experimentation, which the First Amendment places at the heart of political freedom. Richards also raises concerns about governmental surveillance of benign activities because it gives undue power to governmental actors to unfairly classify, abuse, and manipulate those who are being watched; but it is clear that his driving concern is with intellectual privacy. We think that this focus is too narrow.

According to Richards, due to intellectual records' relationship to First Amendment values, "surveillance of intellectual records — Inter-

---

[29] MAJORITY AND MINORITY STAFF REPORT, *supra* note 26, at 79.

[30] INFORMATION SHARING ENVIRONMENT, http://www.ise.gov/ (last visited May 14, 2013).

[31] Citron & Pasquale, *supra* note 17, at 1453 & n.68.

[32] Danielle Keats Citron, *The Privacy Implications of Deep Packet Inspection*, *in* OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, DEEP PACKET INSPECTION (Mar. 2009), *available at* http://www.priv.gc.ca/information/research-recherche/2009/keats-citron_200903_e.asp.

[33] *Id.* Paul Ohm has carefully made the case for why DPI practices storing email communications would violate electronic surveillance laws. Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417.

[34] *See, e.g.*, Duhigg, *supra* note 2.

[35] *See* Amanda C. Pustilnik, *Neutrotechnologies at the Intersection of Criminal Procedure and Constitutional Law*, *in* THE CONSTITUTION AND THE FUTURE OF CRIMINAL JUSTICE IN AMERICA (John T. Parry & L. Song Richardson eds., forthcoming 2013).

[36] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935 (2013).

net search histories, email, web traffic, or telephone communications — is particularly harmful."[37] Richards argues that governmental surveillance seeking access to intellectual records should therefore be subjected to a high threshold of demonstrated need and suspicion before it is allowed by law.[38] He argues also that individuals ought to be able to challenge in court "surveillance of intellectual activities."[39] Richards further proposes that "a reasonable fear of government surveillance that affects the subject's intellectual activities (reading, thinking, and communicating) should be recognized as a harm sufficient to prove an injury in fact under standing doctrine."[40]

Richards is right to call for the protection of "intellectual privacy."[41] Reflecting his concerns, the U.S. Senate's Permanent Subcommittee on Investigations recently reported internal Department of Homeland Security warnings about agents routinely using fusion centers to collect intelligence on "First Amendment-protected activities lacking a nexus to violence or criminality," including those of religious and political groups.[42] One fusion center instructed law enforcement to collect information on supporters of third-party candidates, including the public movements of cars with bumper stickers supporting Ron Paul and Bob Barr.[43] Expressing the impact of this sort of surveillance on intellectual privacy, one political activist explained that he feared being pulled over by a police officer because of political views expressed by his bumper sticker.[44] Although much fusion center surveillance remains hidden, Richards's concerns are valid and pressing; in the present, as in the past, there can be no doubt that surveillance systems interfere with expressive activities.

Although Richards aptly captures the dangers to intellectual freedom posed by technologically enhanced surveillance, we fear his policy prescriptions are both too narrow and too broad because they focus on "intellectual activities" as a necessary trigger and metric for judicial scrutiny of surveillance technologies.[45] Our concerns run parallel to arguments we have made elsewhere against the so-called "mosaic

---

[37] *Id.* at 1962.

[38] *Id.*

[39] *Id.* at 1963.

[40] *Id.* at 1964.

[41] *See id.* at 1935.

[42] MAJORITY AND MINORITY STAFF REPORT, *supra* note 26, at 36.

[43] *See* Citron & Pasquale, *supra* note 17, at 1458; *see also id.* at 1458–63 (discussing the chilling of expressive activities and risk of erroneous classification of individuals raised by fusion centers' surveillance of religious, political, and racial groups).

[44] T.J. Greaney, *'Fusion Center' Data Draws Fire over Assertions*, COLUMBIA DAILY TRIB., Mar. 14, 2009, at A1, *available at* http://www.columbiatribune.com/news/local/fusion-center-data-draws-fire-over-assertions/article_b929741f-2302-5c1e-bcbd-1bc154375a8f.html.

[45] Richards, *supra* note 36, at 1948.

theory" of quantitative privacy[46] advanced by the D.C. Circuit[47] and four Justices of the Supreme Court in *United States v. Jones*.[48] Our argument there supports our objection here: by focusing too much on *what* information is gathered rather than *how* it is gathered, efforts to protect reasonable expectations of privacy threatened by new and developing surveillance technologies will disserve the legitimate interests of both information aggregators and their subjects.

One reason we are troubled by Richards's focus on "intellectual activities" as the primary trigger for regulating surveillance technology is that it dooms us to contests over which kinds of conduct, experiences, and spaces implicate intellectual engagement and which do not.[49] Is someone's participation in a message board devoted to video games sufficiently intellectual to warrant protection? What about a telephone company's records showing that someone made twenty phone calls in ten minutes' time to a particular number without anyone picking up? Would we consider the route someone took going to the library an intellectual activity? Is it the form of the activity or what is being accomplished that matters most?

Setting aside obvious practical concerns, the process of determining which things are intellectual necessarily raises the specter of oppression. Courts and legislators would be required to select among competing conceptions of the good life, marking some "intellectual" activities as worthy of protection, while denying that protection to other "non-intellectual" activities. Inevitable contests over the content and scope of "intellectual privacy" will be, by their nature, subject to the whims and emergencies of the hour.[50] In the face of terrorist threats, decisionmakers will surely promote a narrow definition of "intellectual privacy," one that is capable of licensing programs like Virtual Alabama and fusion centers. Historically, decisionmakers have limited civil liberties in times of crisis and reversed course in times of peace,[51] but the post-9/11 period shows no sign of the pendulum's swinging

---

[46] David Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. (forthcoming 2013) [hereinafter Gray & Citron, *Quantitative Privacy*]; David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. (forthcoming 2013) [hereinafter Gray & Citron, *Shattered Looking Glass*]; David Gray, Danielle Keats Citron & Liz Clark Rinehart, *Fighting Cybercrime After* United States v. Jones, 102 J. CRIM. L. & CRIMINOLOGY (forthcoming 2013).

[47] *See* United States v. Maynard, 615 F.3d 544, 565 (D.C. Cir. 2010).

[48] 132 S. Ct. 945 (2012); *see id.* at 956 (Sotomayor, J., concurring).

[49] *See* Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 110 MICH. L. REV. 311, 330-53 (2012).

[50] Citron & Pasquale, *supra* note 17, at 1479-80 (exploring the Schmittian "state of emergency" exceptionalism embraced in the post-9/11 era).

[51] Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 350 (2008).

back. Given the nature of political and judicial decisionmaking in our state of perpetually heightened security, protection, even of "intellectual privacy," is most likely to be denied to the very outsiders, fringe thinkers, and social experimenters whom Richards is most concerned with protecting.[52]

Richards might argue that his account of "intellectual privacy" and his definition of "intellectual activities" are sufficiently capacious to obviate these concerns. Yet this very capaciousness proves our point. Whether "intellectual privacy" and "intellectual activities" will be read narrowly or broadly, and for that matter, what might constitute a narrow or broad reading, inevitably will be contested just as hotly as the borders of inclusion and exclusion. To draw a loose parallel, the debates among legal positivists and natural law theorists did not abate when Hart expanded the descriptive scope of positivism[53] or when Dworkin did the same for naturalism.[54] To the contrary, they simply expanded the number of battlefronts so that we now see bloody contests within both camps as well as between them.

The Supreme Court has acknowledged the weight of these sorts of concerns in the context of Fourth Amendment debates. For example, in *Kyllo v. United States*, the Court was invited to limit Fourth Amendment protection to activities in the home that can be regarded as "intimate."[55] Writing for the Court, Justice Scalia demurred precisely because he thought the Court had neither the qualifications nor the authority to determine what is and is not "intimate."[56] He therefore focused on the invasiveness of the technology itself — a heat detection device — and its potential to render a wide range of activities in the home, whether "intimate" or not, subject to government surveillance.[57] By our lights, this is a wise path to follow. Although we find persuasive Richards's description of the harms inflicted by totalizing surveillance on intellectual privacy, we are not persuaded that the law should use "intellectual activities" as a trigger for judicial scrutiny or as a special category for judicial treatment any more than the Court should use "intimacy" as a signal for Fourth Amendment regulation.

Rather than assigning primary importance to "intellectual activities" and presumably providing less protection against the acknowl-

---

[52] These concerns — political grudges as well as crisis overreach — animated the Church Commission's support of FISA after the intelligence surveillance abuses of the COINTELPRO era. Brief of Former Church Committee Members and Staff as Amici Curiae Supporting Respondents and Affirmance at 13, 18, Clapper v. Amnesty Int'l USA, No. 11-1025, 2012 WL 4480741, at *13, *18 (U.S. Feb. 26, 2013).

[53] *See generally* H.L.A. HART, THE CONCEPT OF LAW (1961).

[54] *See generally* RONALD DWORKIN, TAKING RIGHTS SERIOUSLY (1977).

[55] Kyllo v. United States, 533 U.S. 27, 37–38 (2001).

[56] *See id.*

[57] *Id.*

edged perils of broader types of surveillance, the law's focus should be on the dangers of totalizing surveillance. Information privacy scholars[58] and surveillance studies theorists[59] alike have long adhered to this approach, and for good reason. Technologies like Virtual Alabama and the fusion-center network amass, link, analyze, and share mass quantities of information about individuals, much of which is quotidian. What is troubling about these technologies is not what information they gather, but rather the broad, indiscriminate, and continuous nature of the surveillance they facilitate.[60] Video cameras may be trained on street corners, drugstore aisles, or a school's bathroom entrances. The information they gather likely does not implicate intellectual activities. They nonetheless create and sustain the kind of surveillance state that is anathema to liberty and democratic culture.[61] Fusion centers rely upon data-broker dossiers, much of which has nothing to do with intellectual endeavors. There is no doubt, however, that continuously streaming all of this information into the information-sharing environment facilitates the sort of broad and indiscriminate surveillance that is characteristic of a surveillance state.

In assessing the privacy interests threatened by such totalizing surveillance, we have in mind some of the lessons taught by Samuel Warren and Louis Brandeis in their foundational article *The Right to Privacy*.[62] Of course, the surveillance technologies of their era could only record discrete slices of life. Nonetheless, Warren and Brandeis recognized that emerging surveillance capacities threatened individuals' interests in being "let alone" in their "private life, habits, acts, and relations."[63] In Warren and Brandeis's view, the watchful eye of "any other modern device for recording or reproducing scenes or sounds" interfered with the development of a person's "inviolate personality."[64] In discussing a husband's note to his son that he did not dine with his wife — a pedestrian communication by any measure — Warren and Brandeis explained that the privacy interest protected was "not the intellectual act of recording the fact that the husband did not dine with

---

[58] *See, e.g.*, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF 141 (2012); Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 195 (2008).

[59] *See, e.g.*, Kevin D. Haggerty, *Tear Down the Walls: On Demolishing the Panopticon*, *in* THEORIZING SURVEILLANCE 23 (David Lyon ed., 2006); David Lyon, *From Big Brother to the Electronic Panopticon*, *in* THE ELECTRONIC EYE 57 (1994); Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498 (1988).

[60] Gray & Citron, *Quantitative Privacy*, *supra* note 46, at 8 & n.45. We are inspired to use this formulation by Susan Freiwald. *See* Susan Freiwald, The Four Factor Test (2013) (unpublished manuscript), *available at* http://works.bepress.com/context/susan_freiwald/article/1012/type/native/viewcontent.

[61] *See generally* Gray & Citron, *Quantitative Privacy*, *supra* note 46.

[62] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[63] *Id.* at 193, 216.

[64] *Id.* at 205–06.

his wife," but the unwanted observance of the "domestic occurrence" itself.[65] Of course, these are precisely the concerns echoed by Justice Scalia on behalf of the Court in *Kyllo*.[66]

The threat posed by contemporary surveillance technologies lies in how much and how often people are watched. Modern technologies allow observers to detect, gather, and aggregate mass quantities of data about mundane daily acts and habits as well as "intellectual" ones.[67] The continuous and indiscriminate surveillance they accomplish is damaging because it violates reasonable expectations of *quantitative* privacy, by which we mean privacy interests in large aggregations of information that are independent from particular interests in constituent parts of that whole.[68] To be sure, the harms that Richards links to intellectual privacy are very much at stake in recognizing a right to quantitative privacy. But rather than being a function of the kind of information gathered, we think that the true threats to projects of self-development and democratic culture lie in the capacity of new and developing technologies to facilitate a surveillance state.

In adopting this view, we ally ourselves in part with commitments to a quantitative account of Fourth Amendment privacy promoted by at least five Justices of the Supreme Court last Term in *United States v. Jones*.[69] In *Jones*, police officers investigating drug trafficking in and around the District of Columbia attached a GPS-enabled tracking device on defendant Jones's car. By monitoring his movements over the course of a month, investigators were able to document both the patterns and the particulars of his travel, which played a critical role in his ultimate conviction. Although the Court resolved *Jones* on the narrow grounds of physical trespass, five justices wrote or joined concurring opinions showing sympathy for the proposition that citizens hold reasonable expectations of privacy in large quantities of data, even if they lack reasonable expectations of privacy in the constitutive parts of that whole.[70] Thus, they would have held that Jones had a reasonable expectation in the aggregate of data documenting his public movements over the course of four weeks, even though he did not have any expectation of privacy in his public movements on any particular afternoon.[71]

---

[65] *Id.* at 201.

[66] Kyllo v. United States, 533 U.S. 27, 37–38 (2001) (Fourth Amendment is concerned with protecting sanctity of the home, not with protecting certain domestic activities over others).

[67] Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1832–33 (2010).

[68] *See* Gray & Citron, *Quantitative Privacy*, *supra* note 46.

[69] 132 S. Ct. 945 (2012).

[70] *Id.* at 956 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring in the judgment).

[71] *See id.* at 964 (Alito, J., concurring in the judgment).

The account of quantitative privacy advanced by the *Jones* concurrences has much in common with the views promoted by Warren and Brandeis. Specifically, the concurring Justices in *Jones* expressed worry that by "making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track," programs of broad and indiscriminate surveillance will "chill[] associational and expressive freedoms," and "alter the relationship between citizen and government in a way that is inimical to a democratic society."[72] Their concerns are well-grounded in original understandings of the Fourth Amendment.[73] As Professor William Stuntz has shown, the Fourth Amendment was drafted partly in reaction to eighteenth-century cases involving the British government's use of general warrants to seize personal diaries and letters in support of seditious-libel prosecutions that were designed to suppress political thought.[74] Despite these roots, quantitative privacy is just beginning to receive recognition because it is only now under threat of extinction by technologies like Virtual Alabama and fusion centers.

There are two ways we might seek to protect quantitative privacy in an age of expanding surveillance technology. One strategy would focus on the aggregations of information assembled with respect to a particular person. This "mosaic" approach presents serious practical concerns along the lines we described with regard to intellectual privacy.[75] As Professor Orin Kerr asks, where would we draw the line between aggregations that are and are not too invasive?[76] How would we treat discrete aggregations assembled by different actors if the sum of those wholes would cross the invasiveness threshold, wherever it is drawn?[77] More importantly, we do not see how this approach could actually preserve reasonable expectations of quantitative privacy. The harm is done, after all, by being watched in a totalizing way — or by the awareness that one might be so watched.[78] Limiting the scope of information dossiers does little to address those concerns. In light of these challenges, we have argued elsewhere for regulating the technologies themselves.[79] Our arguments there strongly suggest that Ri-

---

[72] *Id.* at 956 (Sotomayor, J., concurring) (internal quotation marks omitted).

[73] *See generally* Gray & Citron, *Quantitative Privacy*, *supra* note 46.

[74] William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 394 (1995).

[75] For an extended discussion of the mosaic theory, see Gray & Citron, *Shattered Looking Glass*, *supra* note 46.

[76] Kerr, *supra* note 44, at 333–36.

[77] *Id.*

[78] *See generally* Gray & Citron, *Shattered Looking Glass*, *supra* note 46.

[79] Gray & Citron, *Quantitative Privacy*, *supra* note 46.

chards's goal of protecting intellectual privacy would also be better served by adopting a technology-centered approach.

Of course, none of this argument is intended to discount the benefits of surveillance to national security, criminal justice, emergency response, public administration, or medical care.[80] As Richards observes, any account of surveillance's privacy harms is often resisted on the grounds that some surveillance is essential for the public good. But there is a line between surveillance that is essential for the public good and invasive total-information awareness technologies, and that line is easy to cross if unattended. This leaves us with the question of how to protect society from the gradual acceptance and institutionalization of total-information awareness technologies. Richards supports allowing individuals to challenge surveillance of intellectual activities in court as a cognizable harm. Here again, we worry that his proposal is unlikely to preserve the fundamental interests at stake.

Richards proposes to grant individuals standing to challenge governmental surveillance.[81] Putting concerns about the constitutionality of such a challenge aside, his proposal may raise practical problems. Granting individuals standing to challenge governmental surveillance of them would overwhelm the courts. There are not enough judicial resources to adjudicate three hundred million such suits, each of which could be renewed — almost as soon as it is resolved — on nothing more than suspicion of continued surveillance because the focus, under Richards's approach, is on what information is being gathered. The possibility of a class action would not help matters because individual issues of harm attached to what particular information is gathered would predominate.[82] Suits are also bound to be met with claims of national security interest, to which courts routinely show considerable deference.[83] For example, in litigation involving police surveillance of protestors at the 2004 Republican National Convention, the Second Circuit refused to allow discovery of officers' field reports, even in redacted form, because they would reveal information about undercover operations and thus potentially hinder future ones.[84]

What is more, lawsuits designed to uncover surveillance of intellectual activities may be unable to identify the "intellectual records" gathered by government due to the way certain surveillance systems op-

---

[80] Gray, Citron & Rinehart, *supra* note 46.

[81] This proposal would of course need to overcome or distinguish itself from the Supreme Court's recent decision in *Clapper v. Amnesty Int'l USA*, No. 11-1025, 2013 WL 673253 (U.S. Feb. 26, 2013).

[82] FED. R. CIV. P. 23(b)(3).

[83] David Kravets, *Courts, Congress Shun Addressing Legality of Warrantless Eavesdropping*, WIRED (Jan. 29, 2010, 4:00 PM), http://www.wired.com/threatlevel/2010/01/legality-of-warrantless-eavesdropping/.

[84] *In re* City of New York, 607 F.3d 923, 928 (2d Cir. 2010).

erate. Fusion centers, for instance, may access and analyze private and public databases and real-time video feeds without ever creating and storing records. Although fusion center surveillance of all individuals' on and offline activities is continuous and totalizing, it does not necessarily produce records that could be packaged and produced as part of a discovery process. Ultimately, the vastness of contemporary governmental total-information awareness renders the judiciary incapable of reviewing the majority of situations on an individual basis. Furthermore, any individual cases that made it to judgment could no more chip away at discrete instances of governmental surveillance. Because they would focus on the intellectual privacy interests of specific litigants, these cases would not and could not challenge the system of totalizing surveillance as a whole.

Here again, we think that a technology-centered approach that seeks to protect quantitative privacy is far more promising. Not only would it avoid the constitutional and practical challenges of individual litigation based on the trigger and metric of intellectual privacy, a focus on the technology would also open the door to a wide range of alternative regulatory frameworks that could more efficiently and reliably strike a reasonable compromise between the legitimate interests of government and the privacy interests of citizens.[85] For example, an independent board of experts, such as the Privacy and Civil Liberties Oversight Board (PCLOB), could perform an analysis of the privacy and civil liberties risks posed by surveillance technologies.[86] PCLOB, now fully staffed,[87] could mandate safeguards for the use of surveillance technologies that raise the specter of a surveillance state and make recommendations based on their privileged access to security analyses, piercing the veil secrecy that Richards laments.[88] Board members, vetted for top-secret national security clearances, could attain a comprehensive view of domestic surveillance technologies that

---

[85] Gray & Citron, *Quantitative Privacy*, *supra* note 46.

[86] The PCLOB is an independent agency established by Congress to advise the President and other executive branch officials on matters concerning the protection of privacy. *See* Danielle K. Citron, *Needed Steps Forward on the Privacy and Civil Liberties Oversight Board*, CONCURRING OPINIONS (Jan. 12, 2012, 11:30 AM), http://www.concurringopinions.com/archives/2012/01/needed-steps-forward-on-the-privacy-and-civil-liberties-oversight-board.html.

[87] After years of vacancy, in August 2012 the Senate unanimously confirmed four of President Obama's nominees to PCLOB: Rachel Brand, Elisabeth Cook, Jim Dempsey, and Judge Patricia Wald. Michael Daniel et al., *Senate Confirms Four Nominees to Privacy & Civil Liberties Board*, OSTP BLOG (Aug. 3, 2012, 4:55 PM), http://www.whitehouse.gov/blog/2012/08/03/senate-confirms-four-nominees-privacy-civil-liberties-board. The President's nominee for the Board's chair, David Medine, was finally confirmed in early May 2013, which means PCLOB is fully operational. *See* Allison Grande, Restored Privacy Board Lends Crucial Eye to Data Practices, LAW360 (May 9, 2013, 9:07 PM), http://www.constitutionproject.org/wp-content/uploads/2013/05/5.9.2013_Law360_SBF_PCLOBChair.pdf

[88] Citron & Pasquale, *supra* note 19, at 1488–89.

would enable them to recommend procedural protections for quantitative privacy to prevent governmental abuse.[89] Such procedural protections would by nature protect the intellectual privacy interests at the heart of Richards's proposal without the drawbacks of using intellectual privacy as a trigger and metric of action.

Although we live in a world of total surveillance, we need not accept its dangers — at least not without a fight. As Richards rightly warns, unconstrained surveillance can be profoundly harmful to intellectual privacy. It would be wrong, however, to conflate symptom and cure. What is most concerning, for us is the rapid adoption of technologies that increasingly facilitate persistent, continuous, and indiscriminate monitoring of our daily lives. Although harms to intellectual privacy are certainly central to our understanding of the interests at stake, it is this specter of a surveillance state that we think ought to be the center of judicial, legislative, and administrative solutions, not the particular intellectual privacy interests of individuals.

[89] *Id.* at 1473. For instance, they could require immutable audit logs that promote governmental interest in national security with a commitment to "watch the watchers" by recording all of the uses of that technology.